UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/580,689	05/30/2000	Arturo Maria	113639	1763

24197 7590 06/02/2004

KLARQUIST SPARKMAN, LLP
121 SW SALMON STREET
SUITE 1600
PORTLAND, OR 97204

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/02/2004

10

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/580,689	MARIA, ARTURO	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 March 2004* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 May 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *8* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 3/16/2004, the following **claims 1-38** are presented for examination.

2. Applicant's arguments, pages 13-14, filed on 3/16/2004, with respect to the rejection of claims 1-38 have been fully considered but they are not persuasive. With respect to claim 1, Applicant argues that Bernhard does not teach the receiving a request to initiate intrusion detection services on a remote computer. Examiner respectfully states that in addition to column 7 in the first Office Action, there are other places where there is an intrusion detection service received, for example (see column 2, lines 25-67 and column 9, lines 13-26). Applicant also argues that Bernhard does not teach installing intrusion detection software on said remote computer via said software agent program. As mentioned in the previous Office Action, the ARMS can be considered a software because it is an executable file or program and performs routines as defined in the dictionary, therefore it meets the recitation as recited in the claim, for example (see column 14, line 45 through column 15, line 22). Furthermore, Bernhard discloses that ARMS are installed via IDS software. The IDS software can be interpreted as a software agent program, (see column 8, line 50 through column 8, line 16). Bernhard also discloses other places that recite executing said intrusion detection software on said remote computer via said software agent program, for example (see column 12, lines 30-41). Claim 15 is rejected for the same reasons mentioned above, for example see also column 5, line 7-28) for the step of

receiving a request to become an intrusion detection platform from a remote network location in claim 15. Claim 23 is also still rejected for the same reasons mentioned above. In addition, Bernhard discloses a network of computers and also discloses intrusion detection server sends a request to execute intrusion detection software to a software agent at least one of said plurality of computers when intrusion detection services are needed based on information contained in said database, for example (see also column 5, lines 6-26, lines 45-67, column 6, lines 23 et seq.). Applicant does not overcome the rejection of claims 1-38. Therefore, claims 1-38 still remain rejected.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3.1 **Claims 1-23 and 27-38** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,275,942 to **Bernhard et al.**.

3.2 **As per claims 1and 30, Bernhard et al.** discloses a method for implementing an intrusion detection system in a network, comprising receiving a request at a software agent program to initiate intrusion detection services on a remote computer (column 7, lines 44-50); installing intrusion detection software on said remote computer via said software agent program (column 7, lines 50-65); and executing said intrusion detection software on said remote computer via said software agent program (column 7, lines 30-37; see also column 5, lines 8-28).

As per claim 15, Bernhard et al. discloses a method for implementing an intrusion detection system on a computer connected to a network, comprising receiving a request to become an intrusion detection platform from a remote network location (column 7, lines 44-50); and executing said intrusion detection software (column 7, lines 30-37; see also column 5, lines 8-28).

As per claim 23, Bernhard et al. discloses a system for detecting intrusions in a computer network comprising: a plurality of computers executing software agents; an intrusion detection server (see column 5, lines 8-28 and figure 1); and a database (column 10, line 59 through column 10 line 61 and figures 1 and 7); wherein said intrusion detection server sends a request to execute intrusion detection software to a software agent at at least one of said plurality

of computers when intrusion detection services are needed based on information contained in said database (column 11, line 54 through column 12).

As per claim 2, Bernhard et al. discloses the limitation of receiving a request to terminate intrusion detection services at said software agent program (column 12, lines 30-41). **Bernhard et al.** further discloses that for particular misuses, the API component of the software can interact with similar network elements by different vendors (see column 6, lines 41-61).

As per claims 3 and 20, Bernhard et al. discloses the limitation of monitoring for fulfillment of a stop condition (see figure 4, see column 4, lines 21-39).

As per claims 4, 13, 19, and 38, Bernhard et al. discloses the limitation of wherein said stop condition is based on network traffic conditions (see column 8, lines 59 et seq.; see column 10, line 51 through column 11, line 21). **Bernhard et al.** further discloses that the system monitors all misuses not limited to the examples (see also column 4, lines 21-48).

As per claims 5, 12, 18, and 37, Bernhard et al. discloses the limitation wherein said stop condition is an expiration time (see column 10, lines 41-50).

As per claims 6 and 31, Bernhard et al. discloses the limitation of receiving notification of a network intrusion (see column 12, lines 30-41).

As per claim 7, Bernhard et al. discloses the limitation of selecting said remote computer from a plurality of eligible computers (see column 15, lines 5-18).

As per claim 8, Bernhard et al. discloses the limitation of wherein said selecting step is accomplished based on a network map (column 5, lines 47-63).

As per claims 9, 29, and 34, Bernhard et al. discloses the limitation of wherein said selecting step is accomplished based on a knowledge base (column 12, lines 30-41).

As per claims 10, 14, 21, and 35, Bernhard et al. discloses the limitation of wherein said request is verified using a cryptographic authentication scheme (column 9).

As per claims 11, 17, and 36, Bernhard et al. discloses the limitation of wherein said request includes a stop condition indicating when to stop executing the intrusion detection software (see column 3, lines 1-10; column 4, line 27 et seq. see also claims). **Bernhard et al.** further discloses that users can specify the frequency of updates.

As per claim 16, Bernhard et al. discloses the limitation of installing intrusion detection software on said computer (column 7, lines 50-65).

As per claim 22, Bernhard et al. discloses the limitation of when said intrusion detection software has ceased executing, un-installing said intrusion detection software (see column 7, lines 50-65 see also column 6, lines 41-61).

As per claim 27, Bernhard et al. discloses the limitation of wherein said database contains information about the plurality of computers (column 10, line 59 through column 10 line 61 and figures 1 and 7).

As per claim 28, Bernhard et al. discloses the limitation of wherein said information includes a map of said computer network (column 5, lines 47-63; column 7, lines 5-9; column 12, line 30 through column 13, line 12).

As per claim 32, Bernhard et al. discloses the limitation of selecting said remote computer from a plurality of eligible computers (see figure 5a).

As per claim 33, Bernhard et al. discloses the limitation of wherein said selecting step is accomplished based on a network map (column 7, lines 5-9).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 24-26** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,275,942 to **Bernhard et al.** in view of US Patent 6,023,586 to **Gainsford et al.**.

4.2 **As per claims 24, Bernhard et al.** substantially discloses the limitation of wherein said intrusion detection server increases the number of said plurality of computers executing intrusion detection software when a network intrusion is detected (see column 2, lines 8-34; column 3, lines 1-20). **Bernhard et al.** discloses that the invention is compatible and allows new automated response well known in the art as well as upgradeable. **Bernhard et al.** further discloses the execution of software on various numbers of computers or vendor response component to an instance of misuse (column 8, lines 23-58 and column 15, lines 5-22). **Bernhard et al.** does not explicitly state increasing the number of said plurality computers. To one skilled in the art, it is apparent that the user can choose any number of computers to execute the software to respond to a misuse. However, **Gainsford et al.** in an analogous art teaches having all distribution or executable software occurring simultaneously when a network intrusion is detected (column 12, lines 50-58). Therefore, it would have been obvious to one of ordinary

skill in the art at the time the invention was made to modify the method of **Bernhard et al.** to increase the number of plurality of computers to execute the software in case of an attack as taught by **Gainsford et al.** . This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Gainsford et al.** so as to assure that the misuse is not permitted in any part of the system.

As per claim 25, Bernhard et al. discloses the limitation of wherein said intrusion detection server changes the number of said plurality of computers executing intrusion detection software when the level of network traffic changes (see column 8, lines 59 et seq.; see column 10, line 51 through column 11, line 21).

As per claim 26, Gainsford et al. discloses the limitation of wherein said intrusion detection server changes the number of said plurality of computers executing intrusion detection software depending on the time of day (column 12, lines 50-67).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are 703-872-9306 for regular communications and 703-872-9306 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

CC

Carl Colin

Patent Examiner

May 28, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100